REMARKS

In the specification, the paragraphs on pages 78 to 80 have been amended to correct a few obvious typographical errors and to conform the specification to the drawings.

In paragraph 3 on page 2 of the Official Action, claims 1 to 9 were rejected under 35 U.S.C. 103(a) as being unpatentable over Best (U.S. Patent No. 4,465,901) in view of Heffner et al. (U.S. Patent No. 6,319,740). Applicants respectfully traverse.

The Official Action cites Best for showing various elements of applicants' claims 1 and 7 but recognizes that "Best does not specifically disclose a metal shielding layer over the memory so that the information stored in the memory cannot be read by visual inspection or probing." However, in addition to failing to disclose a metal shielding layer, Best fails to disclose an electronic circuit chip having protected encryption circuitry that operates in the fashion recited in the applicants' claims. In other words, the applicants' claimed electronic circuit chip will not result merely from combining Best and Heffner. For example, subparagraph 3(a) on page 2 of the Official Action refers to element 167 in FIG. 2 of Best as the memory, but this memory is not in Best's protected electronic circuit chip (crypto microprocessor CMP 16 in FIG. 3, for example constructed as an integrated circuit chip as shown in Best's FIG. 15). Subparagraphs 3(d) and 3(e) of the Official Action refer to Best column 7, line 60 – col. 8, line 4 and col. 7, lines 45-47 for encryption circuitry (enciphering circuit 142 in FIG. 19 or a microprogram to encipher data output to random-access memory 151), but it is not clear that the data being enciphered is data from at least one input to the electronic chip; instead, the data is said to

be for "temporary external storage of portions of partially processed data without compromising its contents." (Best, col. 7, lines 48-49.)

In short, Best's crypto-microprocessor CMP "executes an enciphered program by piecemeal deciphering of enciphered instructions as it need them." (Best, Abstract, lines 2-5; column 3 lines 35-41; column 4, lines 41-46.) In contrast, the electronic circuit chip of applicants' claims is for encrypting the data from said at least one input to the electronic chip according to the encryption procedure assigned to the electronic chip, to produce encrypted data that is transmitted from at least one output from the electronic circuit chip.

Page 3 of the Official Action cites Heffner col. 6, lines 11-31 for disclosing a metal shielding layer over a memory as a coated integrated circuit so that the information cannot be read by visual inspection or probing. Heffner, however, is directed generally to forming a multilayer opaque coating on an integrated circuit or multichip module (MCM) to prevent reverse engineering, and Heffner does not refer to a memory or encryption circuitry. More importantly, Heffner col. 6, lines 11-31 says "the EMI hardening coating 52 shields the IC or MCM 10 (i.e., active circuitry) from adverse affects of EMI." The EMI hardening coating 52 is one of a number of ceramic particle based coatings 28, 50, and 52 over the IC or the MCM 10:

> As with the opaque coating 28, both of the coatings 50 and 52 are formed from ceramic particle based coating compositions that have a chemistry similar to the chemistry of the materials of the IC or MCM 10, such that attempted removal of the coatings 50, 52, 28 and 15 (if used)

> from the IC or MCM 10 (for inspection and/or reverse engineering of the topology of the IC or MCM) via chemical methods will simultaneously destroy the IC or MCM 10. As with the coating composition 33, the coating compositions from which the coatings 50 and 52 may be a single chemical component or a multi chemical component compositions. The composition of the radiation coating 50 may be any one of barium titanate, lead oxide, tungsten carbide, bismuth oxide or other heavey [*sic.*] metal compounds. In one preferred embodiment, barium titanate was found to provide a desirable composition for the radiation coating 50. The composition of the EMI coating 52 may be any one of titanium monoxide, chromium carbide, zinc, copper or other conductive metals. In one preferred embodiment, titanium monoxide was found to provide a desirable composition for the EMI coating 52.
>
> Since the coating compositions of the coatings 50 and 52 are ceramic particle based like the coating composition 33 of the opaque coating 28, each coating 50 and 52 can be applied by the thermal spray process 29 (parameters and technique) discussed above, with the form of the compositions for the coatings 50 and 52 (e.g., sintered rod), particle size ranges (i.e., ten to sixty microns with 10 to twenty microns being preferred), application temperature range (i.e., 200° C. to 3000° C), etc., being applicable.

(Heffner, FIG. 3, and col. 6, lines 10-39.)

In contrast, the applicants' claims 1 and 7 recite "a <u>metal shielding layer</u> over the memory so that the information stored in the memory cannot be read by visual inspection

or probing." For example, the applicants' specification teaches that the metal shielding layer is an upper layer of metal on the applicants' chip over an EEPROM memory and data path to the memory makes it virtually impossible to recover the key from the memory by probing, inspection, disassembly, or reverse engineering. (Applicants' specification, page 79, lines 7-11.) It is respectfully submitted that a metal layer is different from a ceramic particle based coating composition that includes conductive metal as a constituent.

Considering the differences between the subject matter of claims 1 and 7 and the disclosures of Best and Heffner, it is respectfully submitted that the subject mater of claims 1 and 7 would not have been obvious. Improper hindsight would be needed to pick and choose pieces of two rather complicated references in order to modify and combine them to arrive at the applicants' novel and elegant solution to providing a tamper-resistant identity chip.

New claims 10, 11, and 12 further distinguish the references by explicitly reciting that the electronic circuit chip is a monolithic semiconductor integrated circuit chip, the memory is an electrically erasable and programmable read-only memory, and the metal shielding layer over the memory is an upper layer of metal on the electronic circuit chip. In other words, these new claims define a re-programmable tamper-resistant circuit chip that does not require any special encapsulation of the chip in or to make it tamper resistant. Support for the new claims is found in the original specification on page 78 line 13 to page 80 line 16 and FIGS. 31 and 32. The complexity of the cited references themselves evidence a long felt but unsolved need to provide such an identity chip that does

not require any special encapsulation of the chip in order to make it tamper resistant.

In view of the above, reconsideration is respectfully requested, and early allowance is earnestly solicited.

Respectfully submitted,

Richard C. Auchterlonie
Reg. No. 30,607
Attorney for Assignee
HOWREY SIMON ARNOLD & WHITE, LLP.
P.O. Box 4433
Houston, Texas 77210
(713) 787-1400

Date: 10 Feb 2004